FIG. 1

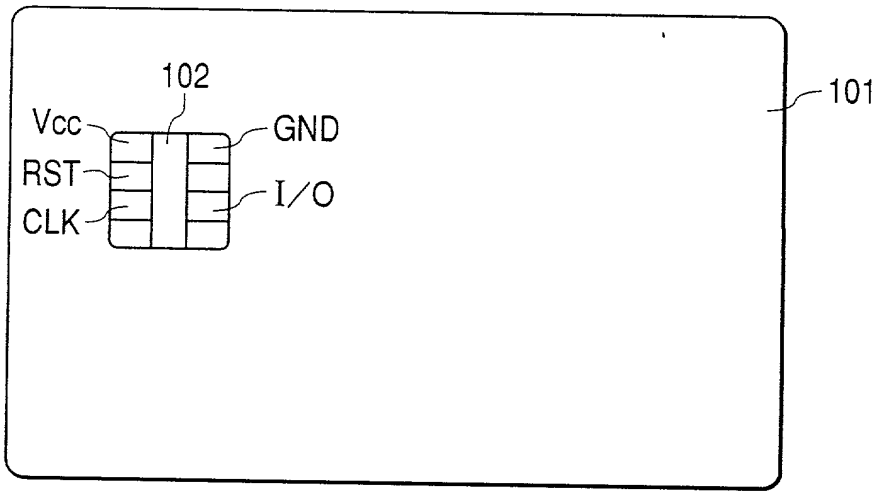

102
Vcc
RST
CLK
GND
I/O
101

FIG. 2

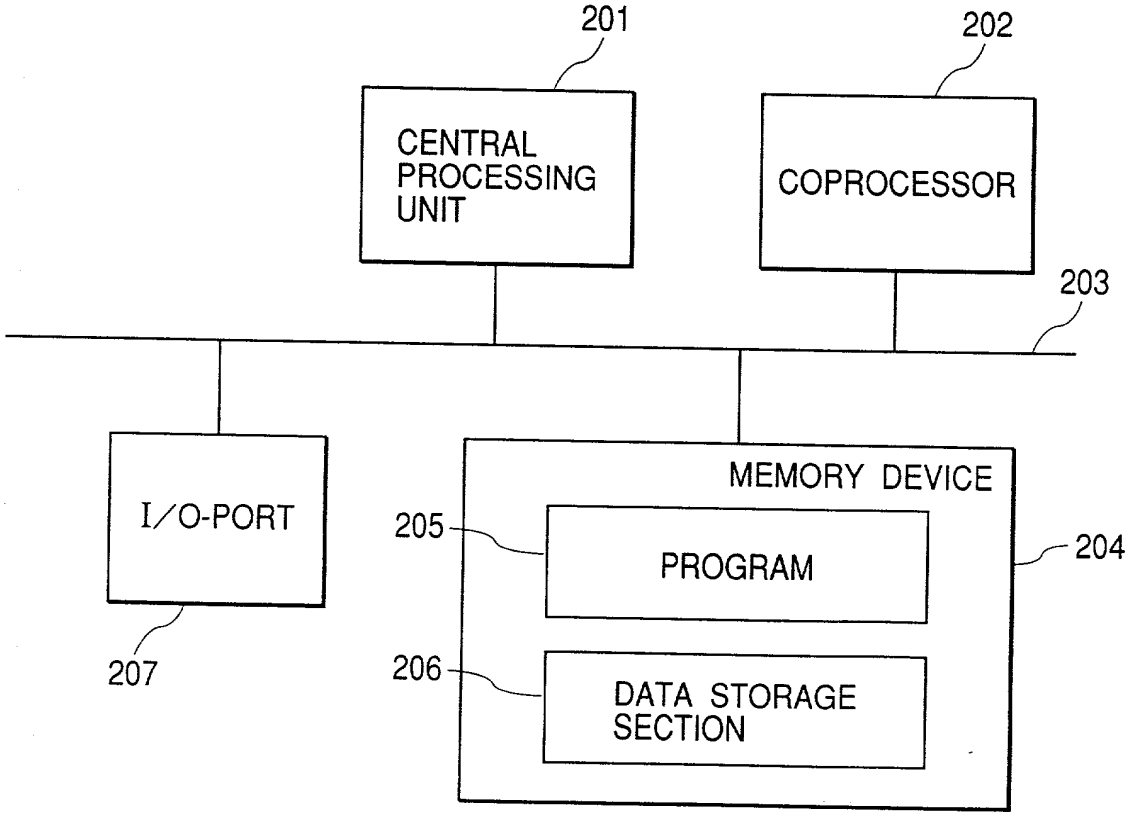

201
CENTRAL PROCESSING UNIT
202
COPROCESSOR
203
I/O-PORT
207
MEMORY DEVICE
205
PROGRAM
204
206
DATA STORAGE SECTION

FIG. 3

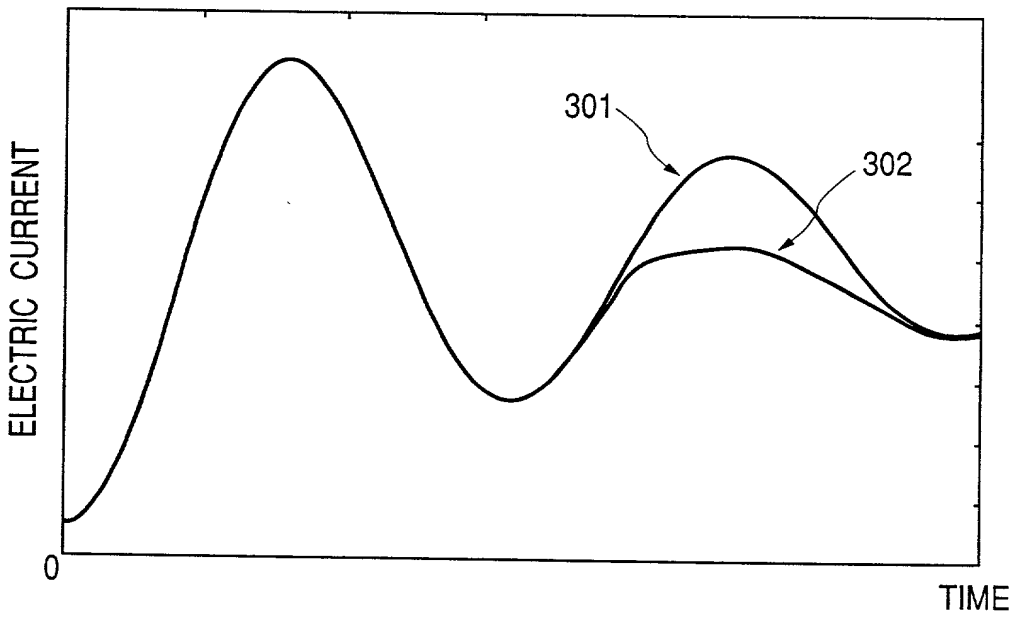


FIG. 4

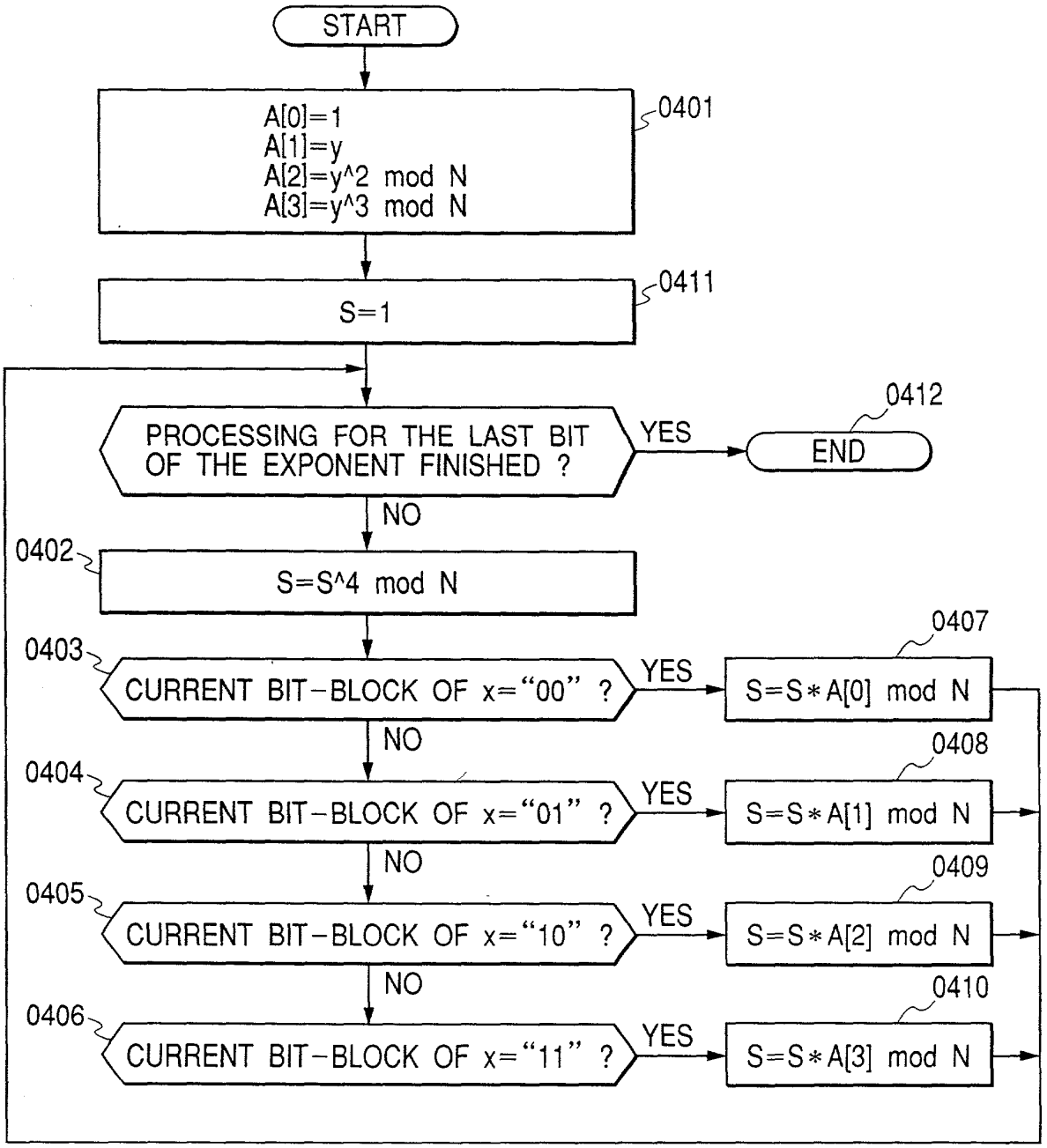

START
A[0]=1
A[1]=y
A[2]=y^2 mod N
A[3]=y^3 mod N
0401
S=1
0411
PROCESSING FOR THE LAST BIT OF THE EXPONENT FINISHED ?
YES
END
0412
NO
0402
S=S^4 mod N
0403
CURRENT BIT-BLOCK OF x="00" ?
YES
S=S*A[0] mod N
0407
NO
0404
CURRENT BIT-BLOCK OF x="01" ?
YES
S=S*A[1] mod N
0408
NO
0405
CURRENT BIT-BLOCK OF x="10" ?
YES
S=S*A[2] mod N
0409
NO
0406
CURRENT BIT-BLOCK OF x="11" ?
YES
S=S*A[3] mod N
0410

FIG. 5

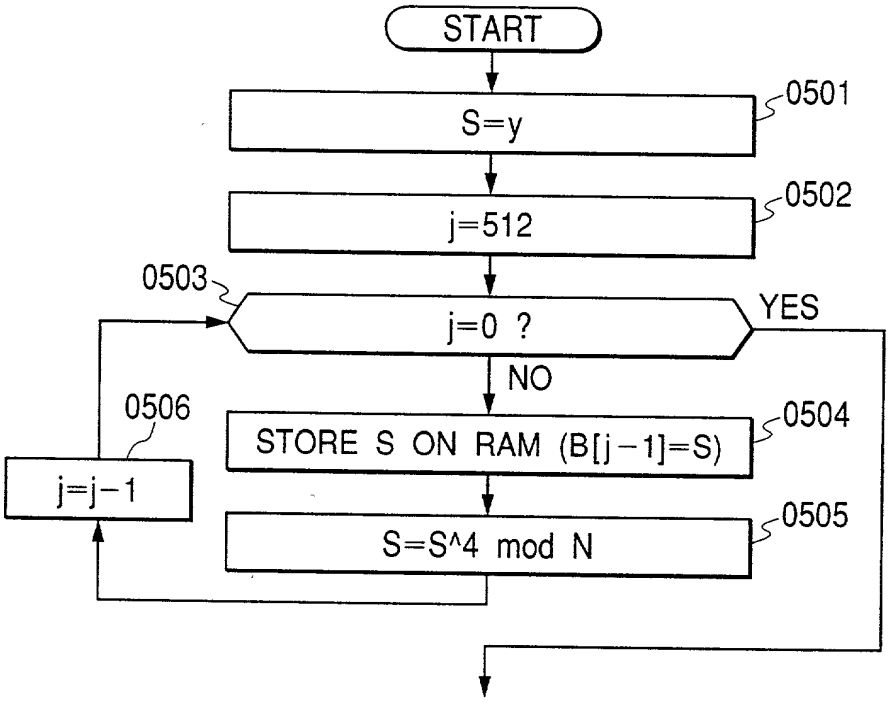

START
S=y
0501
j=512
0502
0503
j=0 ?
YES
NO
0506
STORE S ON RAM (B[j−1]=S)
0504
j=j−1
S=S^4 mod N
0505

FIG. 6

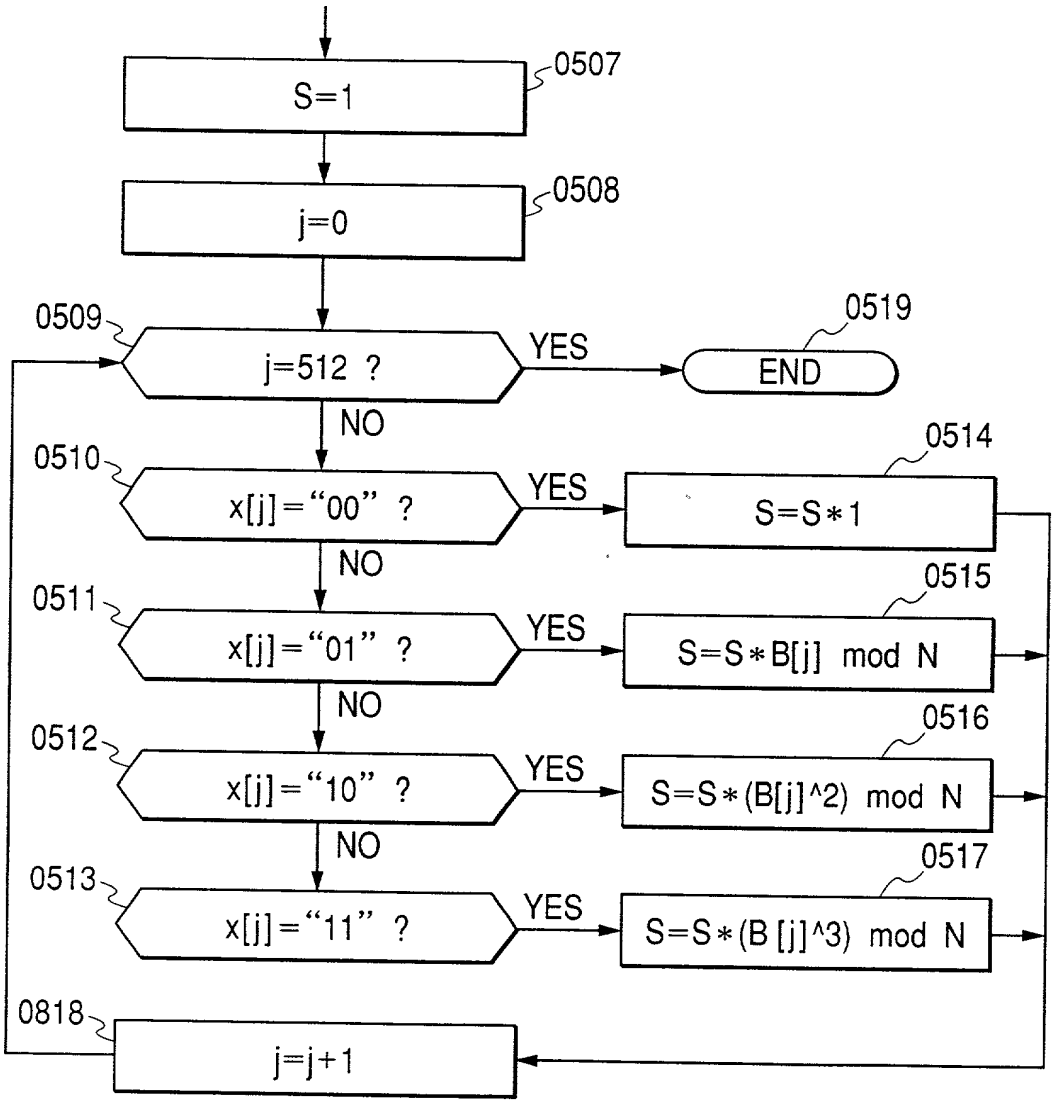

S=1
0507
j=0
0508
0509
j=512 ?
YES
0519
END
NO
0510
x[j]="00" ?
YES
0514
S=S*1
NO
0511
x[j]="01" ?
YES
0515
S=S*B[j] mod N
NO
0512
x[j]="10" ?
YES
0516
S=S*(B[j]^2) mod N
NO
0513
x[j]="11" ?
YES
0517
S=S*(B[j]^3) mod N
0818
j=j+1

FIG. 7

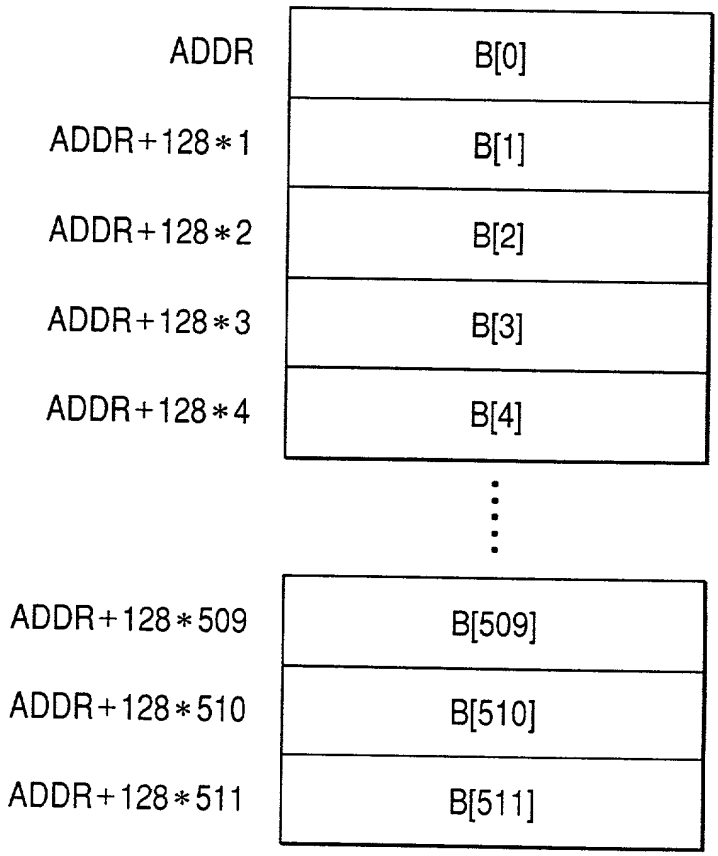

ADDR
B[0]
ADDR+128*1
B[1]
ADDR+128*2
B[2]
ADDR+128*3
B[3]
ADDR+128*4
B[4]
ADDR+128*509
B[509]
ADDR+128*510
B[510]
ADDR+128*511
B[511]

FIG. 8

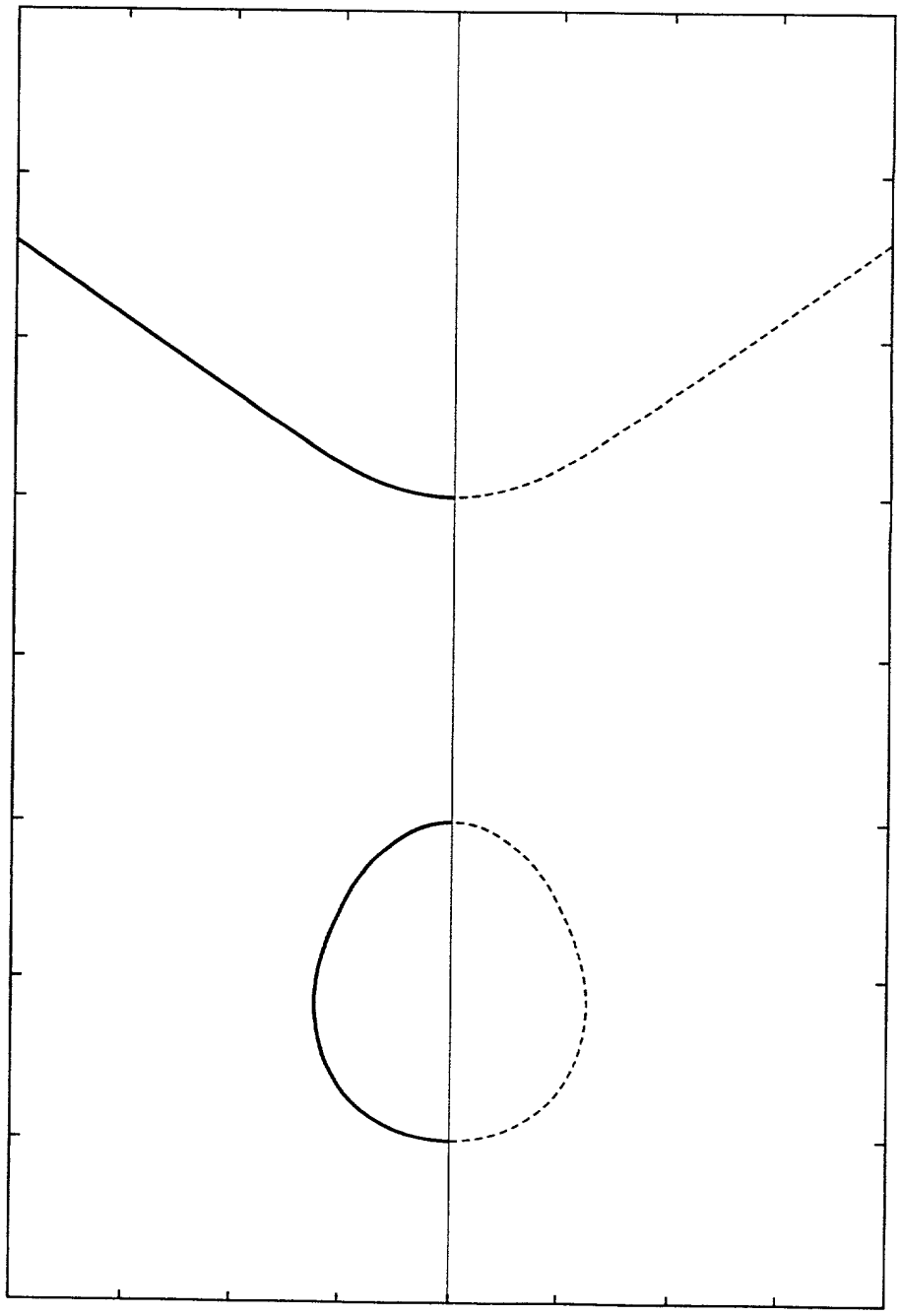


FIG. 9

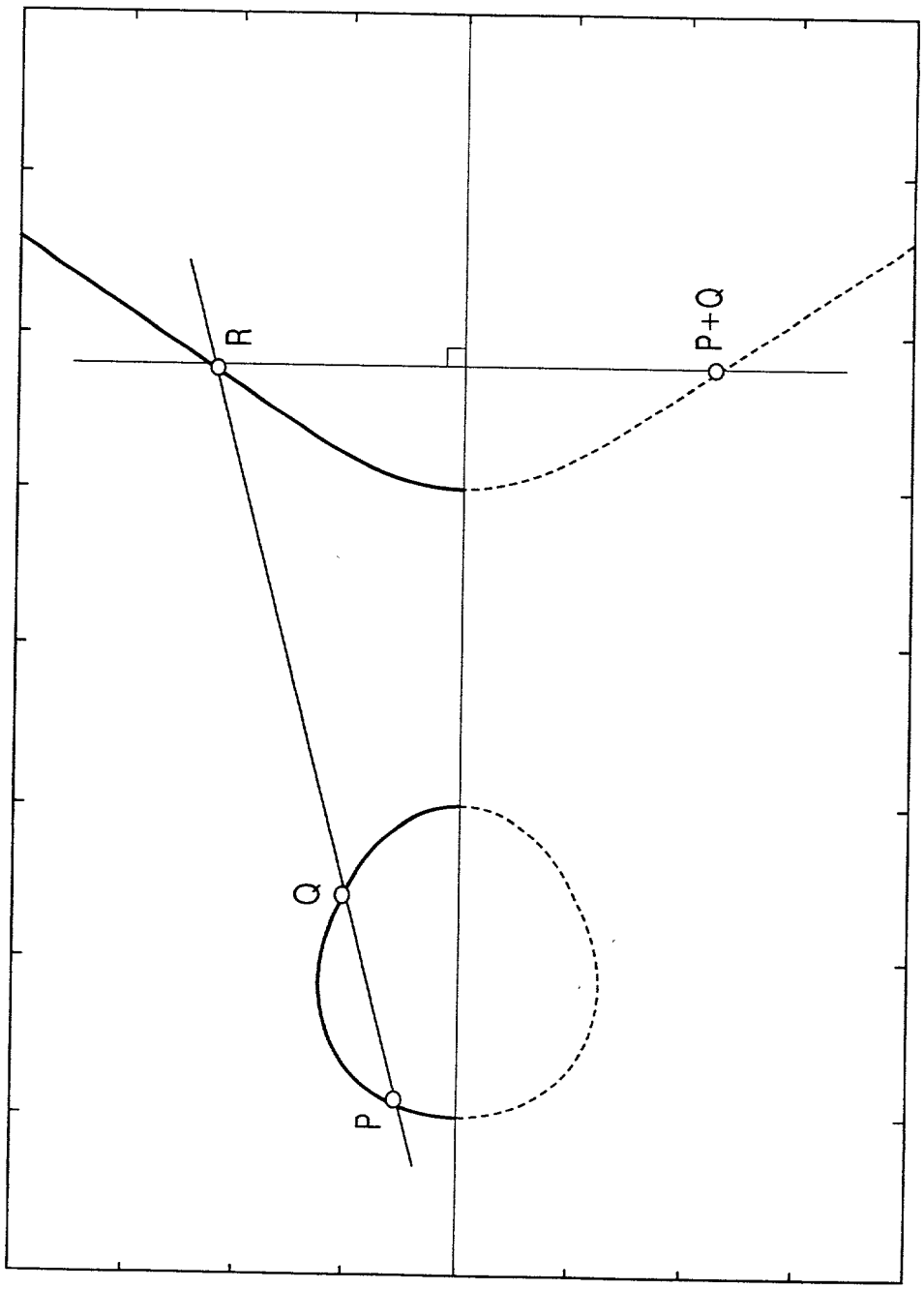


FIG. 10

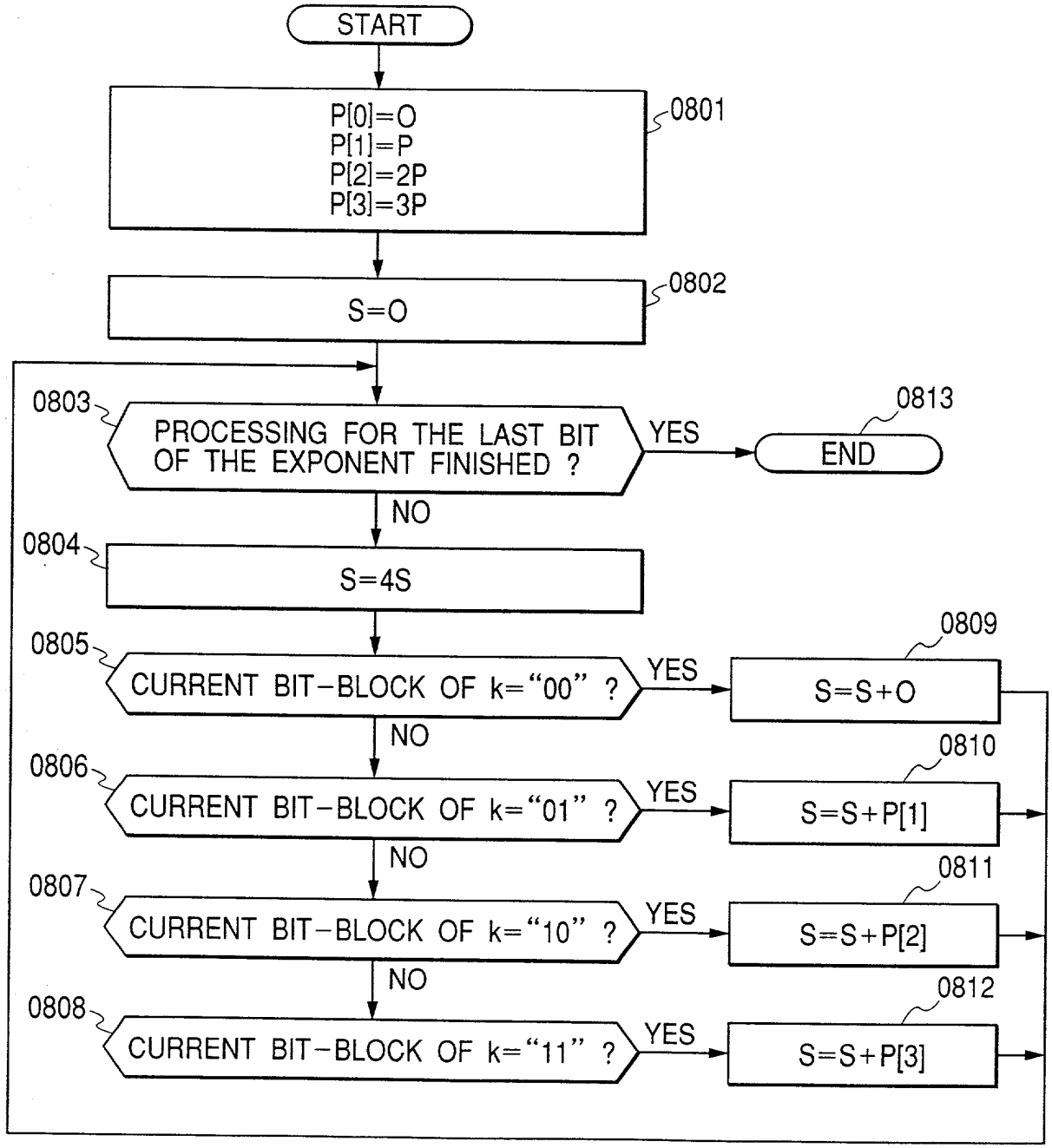

START
P[0]=O
P[1]=P
P[2]=2P
P[3]=3P
0801
S=O
0802
0803
PROCESSING FOR THE LAST BIT OF THE EXPONENT FINISHED ?
YES
0813
END
NO
0804
S=4S
0805
CURRENT BIT-BLOCK OF k="00" ?
YES
0809
S=S+O
NO
0806
CURRENT BIT-BLOCK OF k="01" ?
YES
0810
S=S+P[1]
NO
0807
CURRENT BIT-BLOCK OF k="10" ?
YES
0811
S=S+P[2]
NO
0808
CURRENT BIT-BLOCK OF k="11" ?
YES
0812
S=S+P[3]

FIG. 11

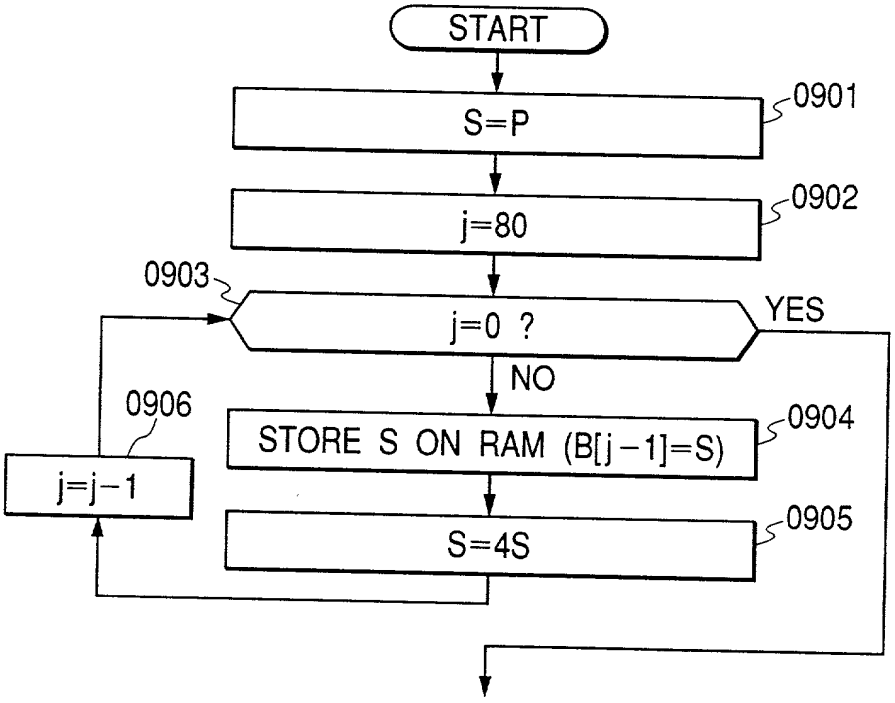

START
S=P
0901
j=80
0902
0903
j=0 ?
YES
NO
0906
STORE S ON RAM (B[j-1]=S)
0904
j=j-1
S=4S
0905

FIG. 12

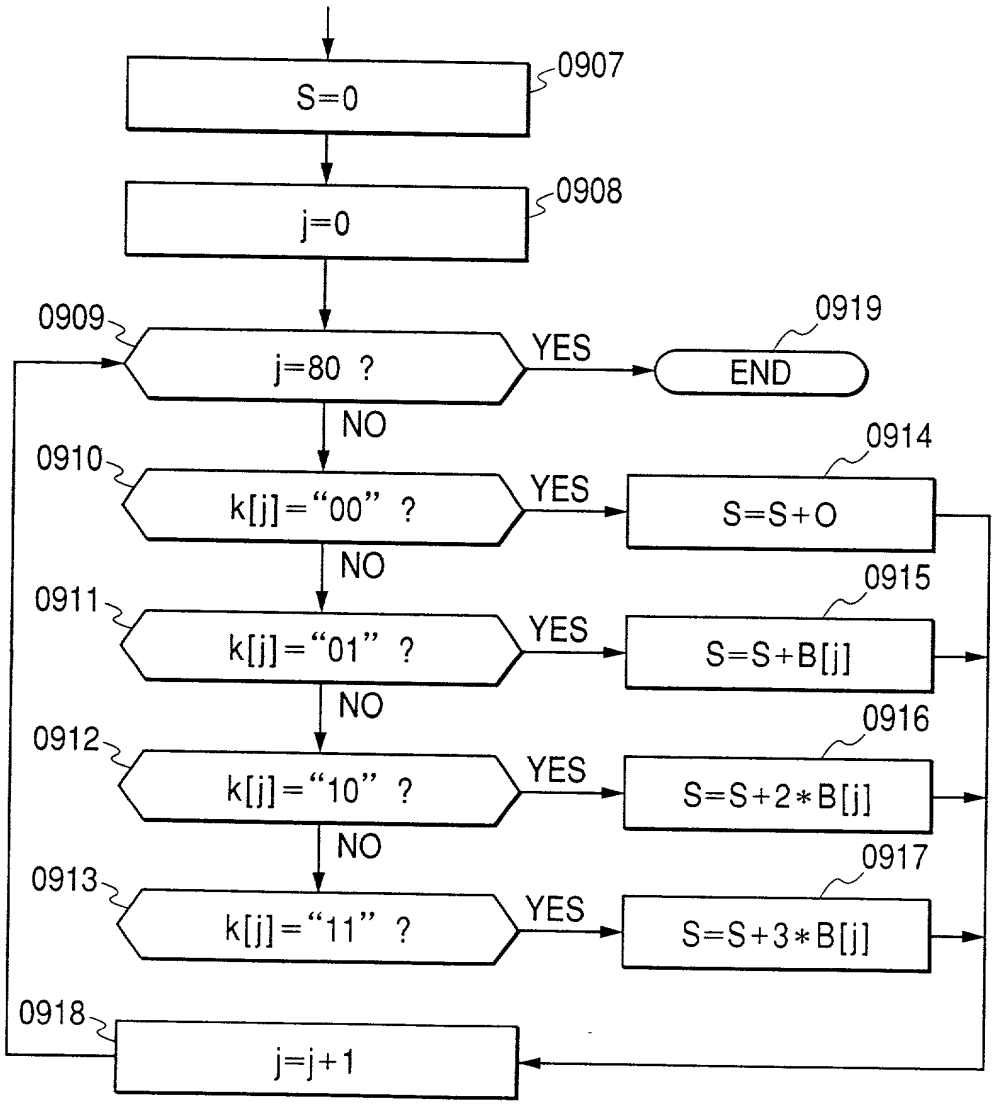

S=0
0907
j=0
0908
0909
j=80 ?
YES
0919
END
NO
0910
k[j]="00" ?
YES
0914
S=S+O
NO
0911
k[j]="01" ?
YES
0915
S=S+B[j]
NO
0912
k[j]="10" ?
YES
0916
S=S+2*B[j]
NO
0913
k[j]="11" ?
YES
0917
S=S+3*B[j]
0918
j=j+1

FIG. 13

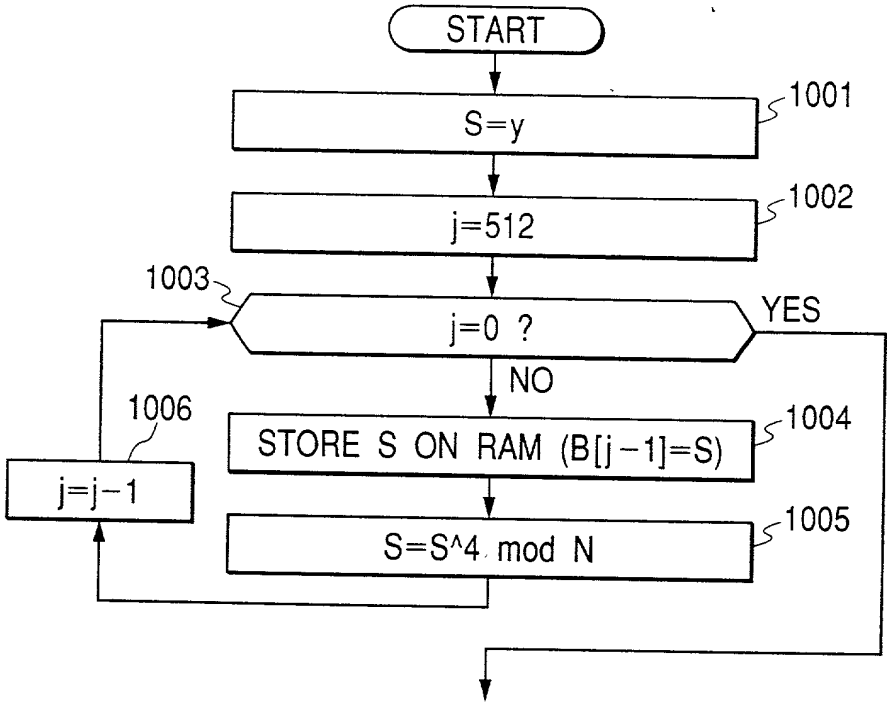

START
S=y
1001
j=512
1002
1003
j=0 ?
YES
NO
1006
STORE S ON RAM (B[j-1]=S)
1004
j=j-1
S=S^4 mod N
1005

FIG. 14

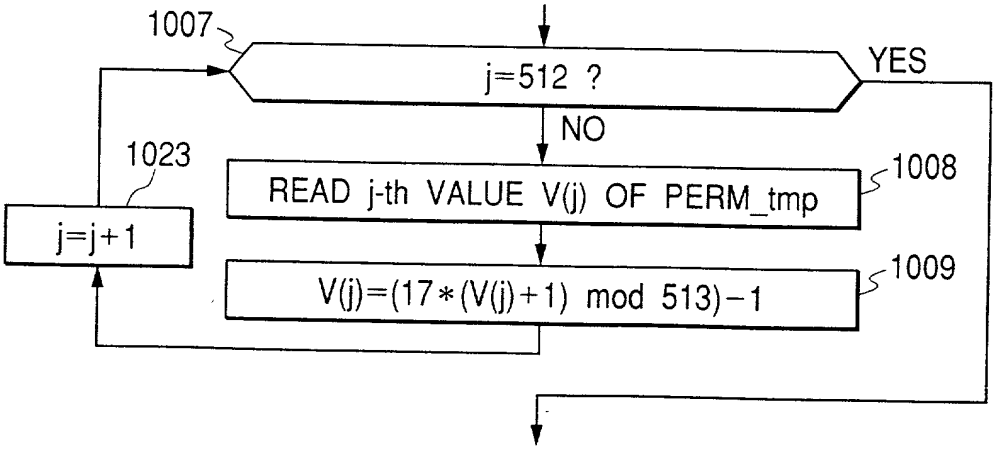

1007
j=512 ?
YES
NO
1023
READ j-th VALUE V(j) OF PERM_tmp
1008
j=j+1
V(j)=(17*(V(j)+1) mod 513)-1
1009

FIG. 15

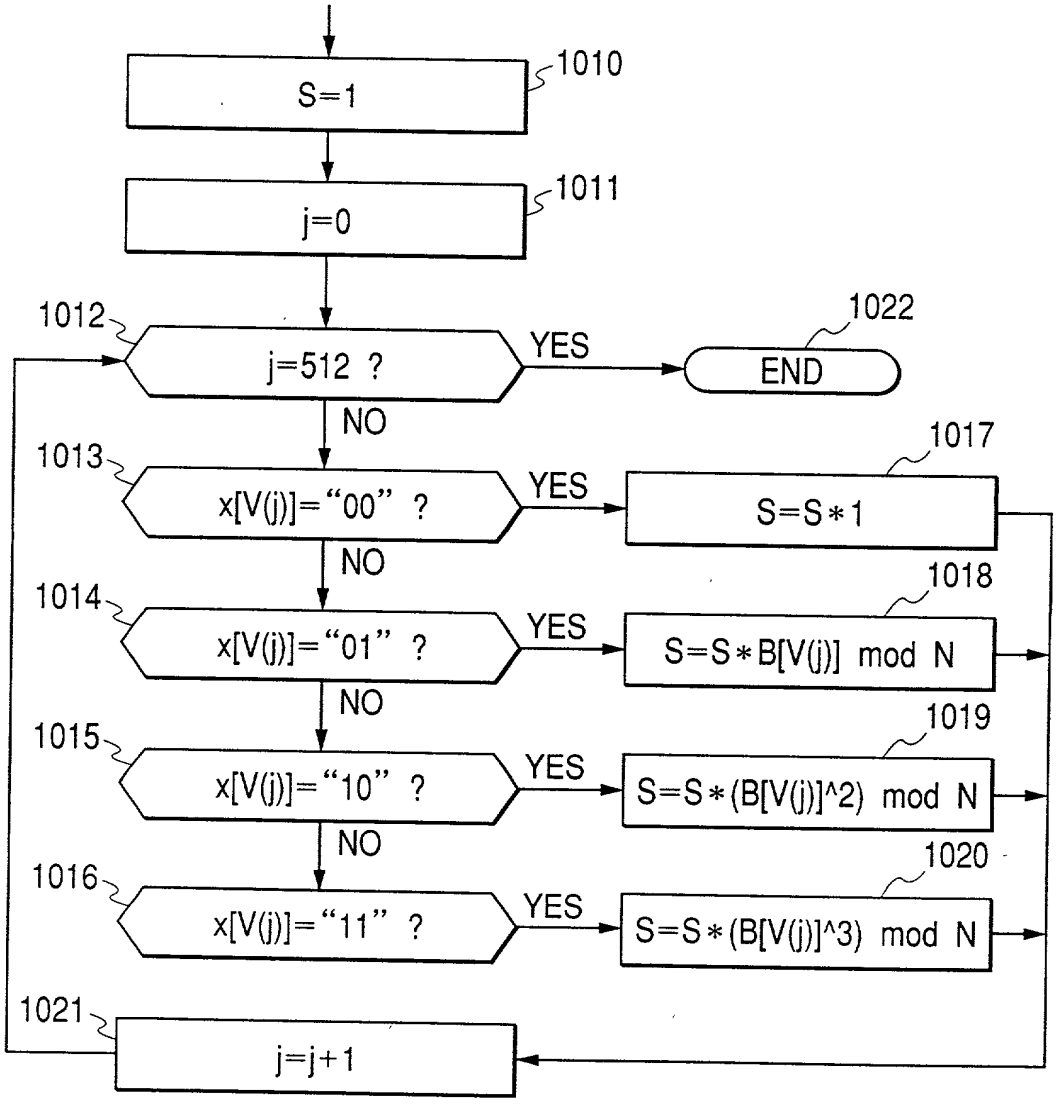

S=1
1010
j=0
1011
1012
j=512 ?
YES
1022
END
NO
1013
x[V(j)]="00" ?
YES
1017
S=S*1
NO
1014
x[V(j)]="01" ?
YES
1018
S=S*B[V(j)] mod N
NO
1015
x[V(j)]="10" ?
YES
1019
S=S*(B[V(j)]^2) mod N
NO
1016
x[V(j)]="11" ?
YES
1020
S=S*(B[V(j)]^3) mod N
1021
j=j+1

FIG. 16

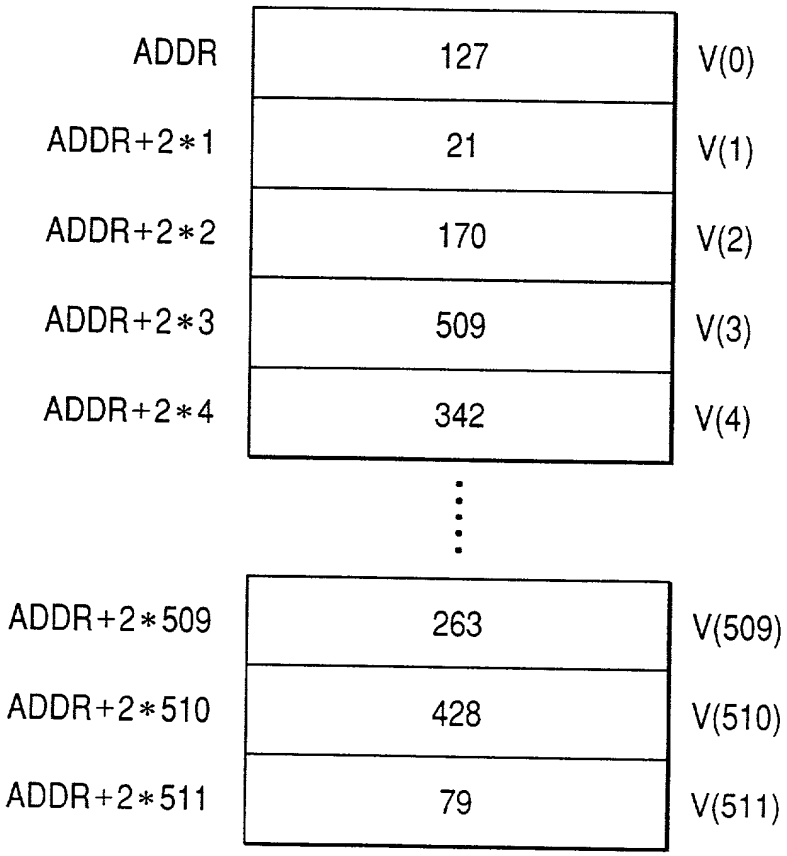

ADDR
127
V(0)
ADDR+2*1
21
V(1)
ADDR+2*2
170
V(2)
ADDR+2*3
509
V(3)
ADDR+2*4
342
V(4)
ADDR+2*509
263
V(509)
ADDR+2*510
428
V(510)
ADDR+2*511
79
V(511)

FIG. 17

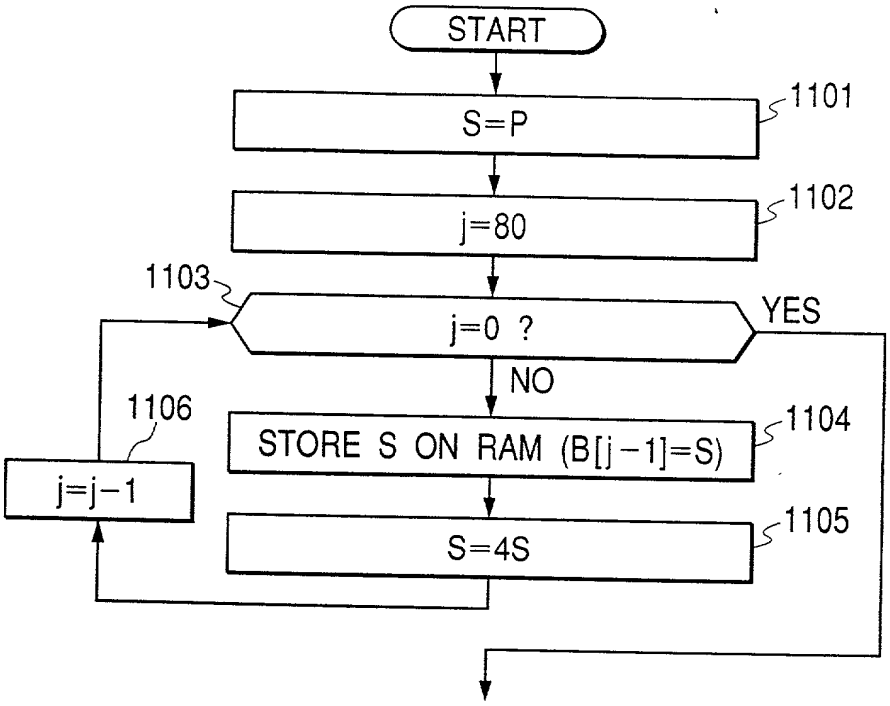

START
S=P
1101
j=80
1102
1103
j=0 ?
YES
NO
1106
STORE S ON RAM (B[j-1]=S)
1104
j=j-1
S=4S
1105

FIG. 18

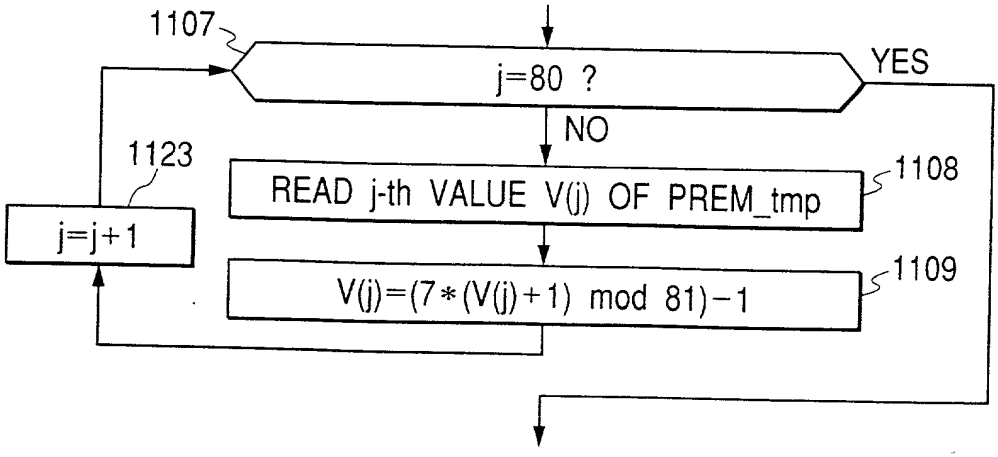

1107
j=80 ?
YES
NO
1123
READ j-th VALUE V(j) OF PREM_tmp
1108
j=j+1
V(j)=(7*(V(j)+1) mod 81)-1
1109

FIG. 19

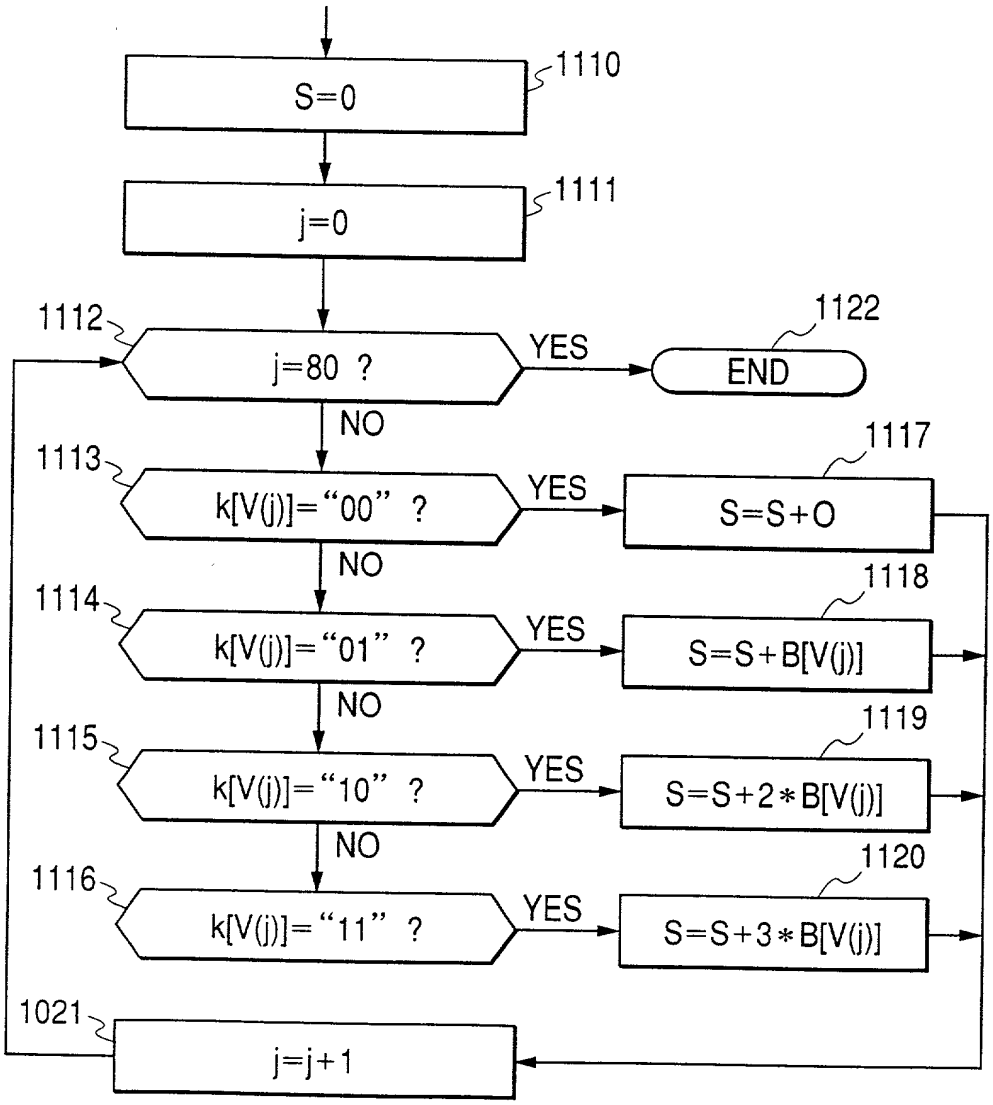

S=0
1110
j=0
1111
1112
j=80 ?
YES
1122
END
NO
1113
k[V(j)]="00" ?
YES
1117
S=S+O
NO
1114
k[V(j)]="01" ?
YES
1118
S=S+B[V(j)]
NO
1115
k[V(j)]="10" ?
YES
1119
S=S+2*B[V(j)]
NO
1116
k[V(j)]="11" ?
YES
1120
S=S+3*B[V(j)]
1021
j=j+1

FIG. 20

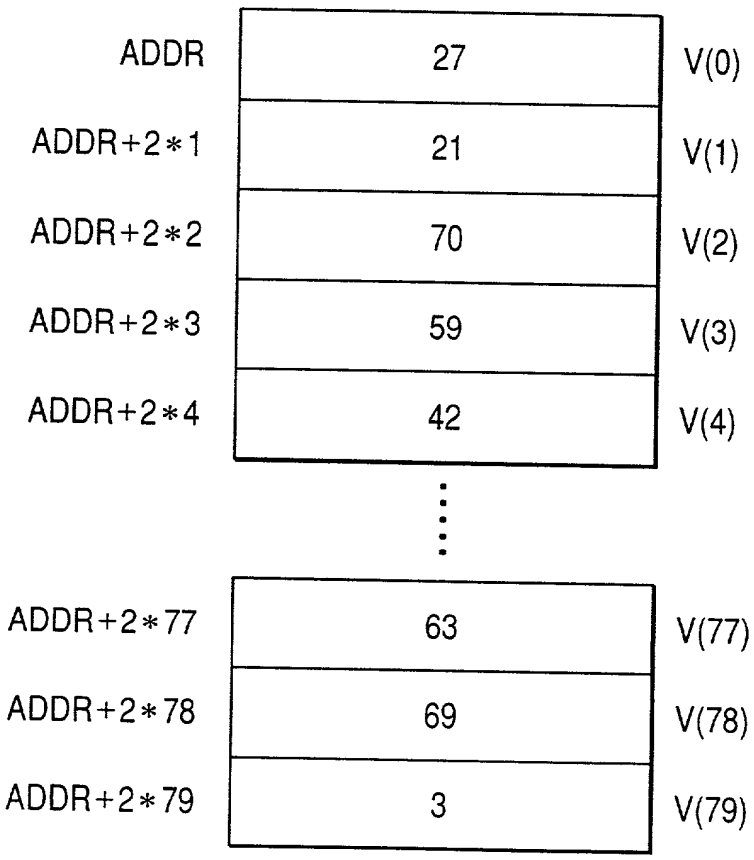

ADDR
27
V(0)
ADDR+2*1
21
V(1)
ADDR+2*2
70
V(2)
ADDR+2*3
59
V(3)
ADDR+2*4
42
V(4)
ADDR+2*77
63
V(77)
ADDR+2*78
69
V(78)
ADDR+2*79
3
V(79)

FIG. 21

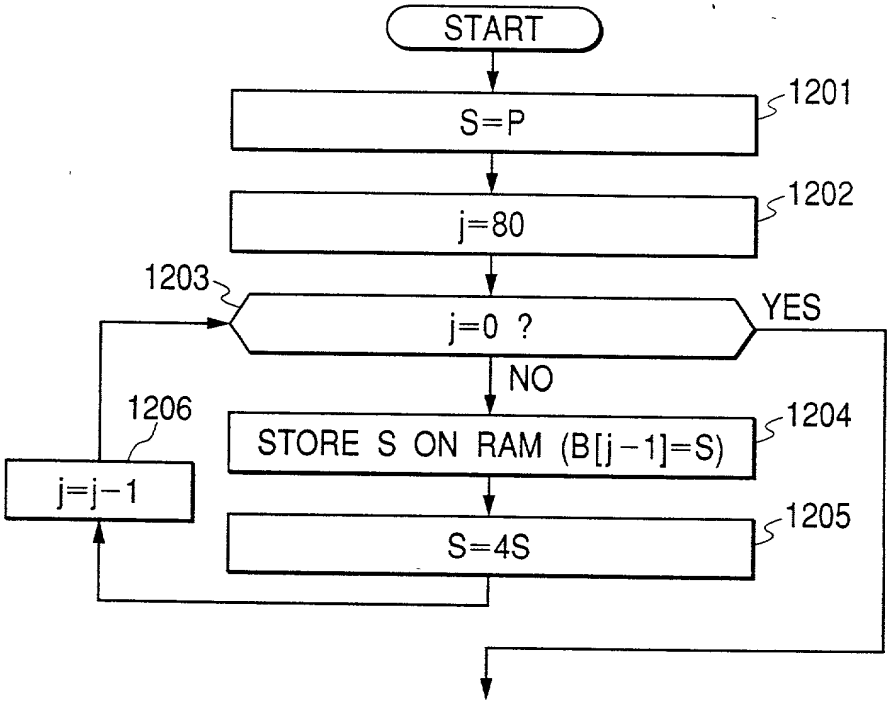

START
S=P
1201
j=80
1202
1203
j=0 ?
YES
NO
1206
STORE S ON RAM (B[j-1]=S)
1204
j=j-1
S=4S
1205

FIG. 22

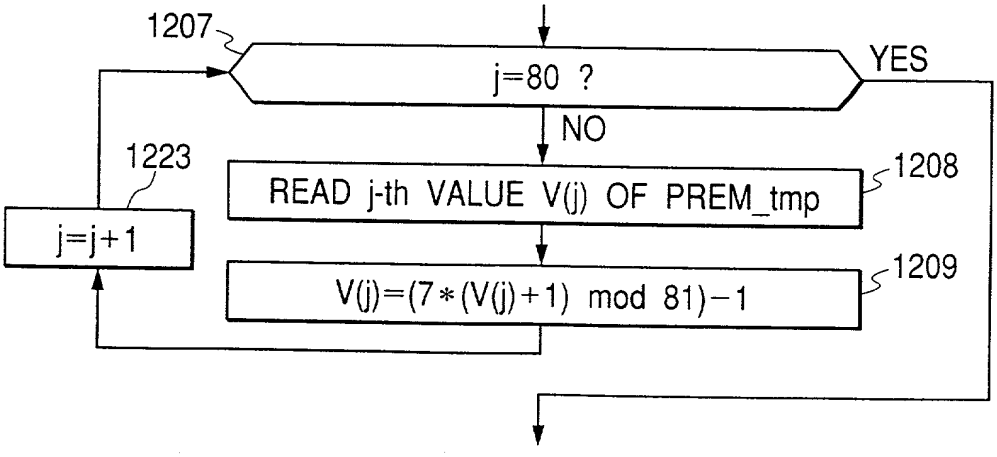
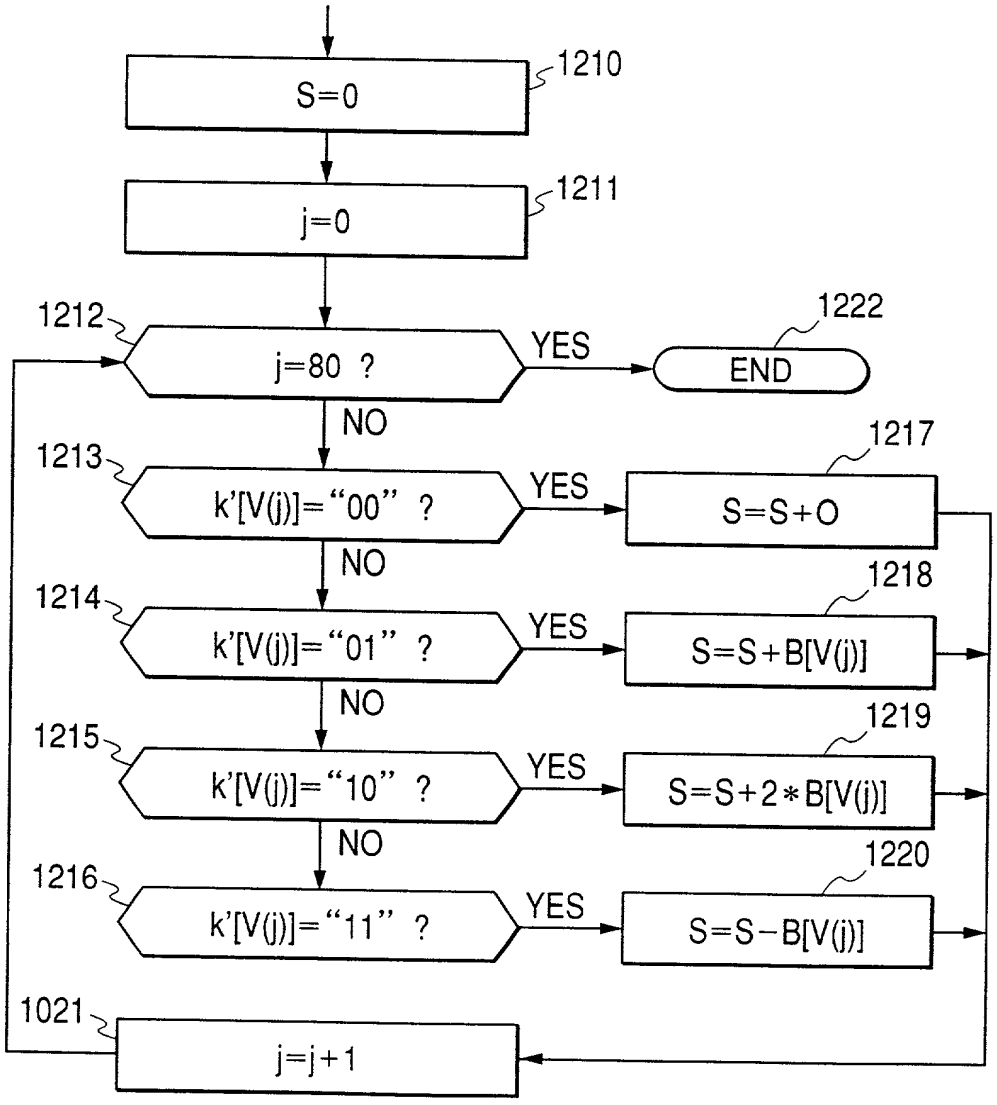

1207
j=80 ?
YES
NO
1223
READ j-th VALUE V(j) OF PREM_tmp
1208
j=j+1
V(j)=(7*(V(j)+1) mod 81)-1
1209

FIG. 23


S=0
1210
j=0
1211
1212
j=80 ?
YES
1222
END
NO
1213
k'[V(j)]="00" ?
YES
1217
S=S+O
NO
1214
k'[V(j)]="01" ?
YES
1218
S=S+B[V(j)]
NO
1215
k'[V(j)]="10" ?
YES
1219
S=S+2*B[V(j)]
NO
1216
k'[V(j)]="11" ?
YES
1220
S=S-B[V(j)]
1021
j=j+1